STATE OF CONNECTICUT

M.JODI RELL
GOVERNOR
EDWIN R. RODRIGUEZ
COMMISSIONER

Department of Consumer Protection

FACT SHEET: How to Defend Against the Privacy Pirates

Consumers are facing an attack on their personal privacy unlike that seen by any earlier generation. Thoroughly shielding your privacy may be close to impossible these days. But it's critical to understand how your privacy can be compromised and the consequences of such a breach — and take a few simple steps to better the odds in your favor.

Identity theft is booming

This broad area includes a number of privacy crimes, including theft of a Social Security number, a credit or debit card, or even the pilfering of phone calling cards. The numbers of identity theft crimes are beginning to add up quickly. A recent government report estimates that as many as 750,000 Americans are victims of identity theft every year. And that number may be low, as many people choose not to report the crime or, for that matter, even know they've been victimized.

In November 1999, the Federal Trade Commission's Identity Theft Data Clearinghouse was fielding about 455 calls a week. Two years later, that number had jumped to more than 3,000. MasterCard and Visa estimate that more than $114 million in credit-card related identity theft occurred in 2000. The government, which has a broader definition of identity theft, puts the number closer to $1 billion now. Victims spend an average of 175 hours per incident trying to unravel the problems caused by identity theft.

How it can happen

A great deal of identity theft still comes down to hands-on mischief — things like "dumpster diving," in which criminals sift through trash to find a credit-card statement or solicitation that someone didn't tear up, and "shoulder surfing," where criminals try to spot calling card and personal identification numbers.

Hoever, eighty percent of victims who call the Federal Trade Commission's Identity Theft Program say they have no idea how it happened.

Officials also acknowledge that the Internet has opened new avenues for theft. If nothing else, the Web allows thieves to send stolen data to most any worldwide location.

One popular scam involves fake mortgage brokers who dangle super low rates if the applicant is quick to provide personal data. Still another uses e-mails in which the sender poses as an Internet service provider asking for information.

A new device called a *skimmer* also poses a threat to consumers. A skimmer is about the size of a credit card, used by a criminal who has cut a deal with a dishonest waiter in a restaurant. When you give the waiter your credit card, he rings it up, but also runs it through the skimmer, which collects your credit card information, which gets passed on to his partner in crime.

A stolen wallet containing a Social Security card lets a criminal quickly set up dummy bank and savings accounts. The very presence of the account may prompt some banks to give the criminal a credit card. From there, the con artist may waste little time maxing out the card, or take a bit more time and build up the card's buying power. That can mean fraudulent purchases as pricey as cars and boats.

Simple ways to protect yourself

There's no ironclad protection that guarantees that you'll never fall victim to some form of identity theft. But there are steps you can take to shield your privacy, many of which are rather simple:

☞ Destroy private records and statements. Tear or shred credit card statements, solicitations and other documents that contain private financial information.

☞ Empty your mailbox quickly so criminals don't have a chance to snatch credit card pitches. Consider locking your mailbox.

☞ Don't carry your Social Security card with you, or any other card that may have your number.

☞ Don't put your social security number on your checks. Leave your driver's license number off your checks as well.

☞ Never leave ATM or gas station receipts behind.

☞ Worried about credit card skimming? Pay with cash as often as possible.

☞ When making an online purchase, look in the lower right hand corner of your browser window. If you see the icon of a lock, that means you're dealing with a secure site. If you don't see one, you'll be safer finding another merchant. Also, check out Web site privacy policies. Shy away from sites that don't specifically say that they won't pass your name and information around to others.

☞ Stick to well-known retailers or sites that others have used to their satisfaction. Use only one credit card for online purchases. That way, if something amiss happens, it'll be easier to spot on your bill.

☞ Be more defensive with personal information. Ask salespeople and others if information such as a Social Security number or driver's license is absolutely necessary. Ask anyone who does require your Social Security number — for instance, your insurance company — what their privacy policy is and whether you can arrange for the organization not to share that information with anyone else.

☞ If you get an unwanted e-mail, don't click the "remove me" option that many such mails offer. In many cases, all that means is that the mail has hit an active address, which only means more solicitations. Use your delete key, and then empty your email trash can.

☞ o Set up a second e-mail address. Use that e-mail address for transactions and other activities that may lead to spams. Use your other address for all private communication.

☞ Besieged by telephone solicitations? Just tell them not to call again. The Telephone Consumer Protection Act of 1991 stipulates that they have to stop calling if you ask. You can also get on the National Do Not Call Registry, operated by the Federal Trade Commission. The web address is: www.donotcall.gov If you do not use the internet, you can register by phone (1-888-382-1222).

☞ Contact your credit card company and find out how to take part in their "opt out" program. This prevents your name from being passed around to solicitors and other companies with whom your cardholder deals.

☞ Check your credit report at least once a year to look for suspicious activity. If you spot something, alert your card company or the creditor immediately.

If something goes wrong

First, contact the fraud departments of each of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, along with a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts.

Equifax
To order a report: 1-800-685-1111
or write: P.O. Box 740241, Atlanta, GA 30374
To report fraud: 1-800-525-6285
and write: P.O. Box 740241, Atlanta, GA 30374

Experian
To order a report: 1-888-EXPERIAN
(397-3742)
or write: P.O. Box 2104, Allen TX 75013
To report fraud: 1-888-EXPERIAN (397-3742)
and write: P.O. Box 9532, Allen TX 75013

TransUnion
To order a report: 800-916-8800
or write: P.O. Box 1000, Chester, PA 19022
To report fraud: 1-800-680-7289
and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

Contact the creditors for any accounts that have been tampered with or opened fraudulently. Speak with someone in the security or fraud department of each creditor, and follow up with a letter.

File a report with your local police or the police in the community where the identity theft took place. Get a copy of the police report in case the bank, credit-card company or others need proof of the crime.

Keep records of everything involved in your efforts to clear up fraud, including copies of written correspondence and records of telephone calls.